View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Ghent University Academic Bibliography

Reversible computation, quantum computation, and computer architectures in between

by Alexis De Vos and Michiel Boes
Imec and Vakgroep elektronika en informatiesystemen
Universiteit Gent
Sint Pietersnieuwstraat 41
B - 9000 Gent, Belgium

and Stijn De Baerdemacker,
Vakgroep fysica en sterrenkunde
Universiteit Gent
Proeftuinstraat 86
B - 9000 Gent, Belgium

***Abstract*—Thanks to the cosine-sine decomposition of unitary matrices, an arbitrary quantum circuit, acting on w qubits, can be decomposed into $2^w - 1$ elementary quantum gates, called controlled V gates. Thanks to the Birkhoff decomposition of doubly stochastic matrices, an arbitrary (classical) reversible circuit, acting on w bits, can be decomposed into $2w - 1$ elementary gates, called controlled NOT gates. The question arises under which conditions these two synthesis methods are applicable for intermediate cases, i.e. computers based on some group, which simultaneously is a subgroup of the unitary group U(2^w) and a supergroup of the symmetric group S_{2^w}. It turns out that many groups either belong to a class that might have a cosine-sine-like decomposition but no Birkhoff-like decomposition and a second class that might have both decompositions. For an arbitrary group, in order to find out to which class it belongs, it suffices to evaluate a function $\Phi(m)$, deduced either from its order (in case of a finite group) or from its dimension (in case of a Lie group). Here $m = 2^w$ is the degree of the group.**

I. Introduction

We consider a quantum circuit acting on w qubits (Fig. 1). We call w the width of the circuit, as the latter has w input qubits and w output qubits. The circuit performs a unitary operation, represented by an $m \times m$ unitary matrix, i.e. a member of the Lie group U(m). Here m stands for 2^w and is called the degree of the circuit.

Each such circuit may be decomposed according to the cosine-sine decomposition: see Fig. 2a. Applying such matrix decomposition again and again leads to the circuit decomposition of Fig. 3a, with $2^w - 1$ control gates. Each box in the figure denotes a controlled 1-qubit

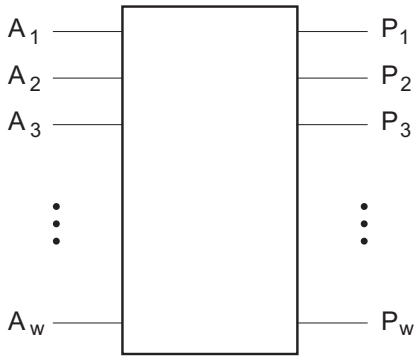

Fig. 1. A circuit of width w.

transformation, i.e. a 2×2 unitary matrix. The actual transformation, however, depends on (i.e. is controlled by) the state of the other $w-1$ qubits. Therefore, the box, in fact, depicts 2^{w-1} matrices of size 2×2, each from the Lie group U(2). Because we denote by V an arbitrary element of U(2), a control gate is also called a controlled V gate. E.g. a contolled V of width 2, the second qubit being controlled by the first one, is represented by a matrix

$$\begin{pmatrix} V'_{11} & V'_{12} & 0 & 0 \\ V'_{21} & V'_{22} & 0 & 0 \\ 0 & 0 & V''_{11} & V''_{12} \\ 0 & 0 & V''_{21} & V''_{22} \end{pmatrix},$$

whereas a contolled V of width 2, where the first qubit is controlled by the second one, is represented by a matrix

$$\begin{pmatrix} V'_{11} & 0 & V'_{12} & 0 \\ 0 & V''_{11} & 0 & V''_{12} \\ V'_{21} & 0 & V'_{22} & 0 \\ 0 & V''_{21} & 0 & V''_{22} \end{pmatrix}.$$

Thus, in a control gate, only one particular qubit is subject to a unitary transformation. The 2×2 matrix representation of the applied transformation is either V' or V'' or V''' or ... or $V^{(2^{w-1})}$, depending on the actual (eigen)state of the other $w-1$ qubits. A control gate thus is a quantum generalization of the classical reversible logic gate known as the controlled NOT, where one particular bit is subject to either of the two 2×2 matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} ,$$

depending of the actual values of the other $w-1$ bits.

Classical reversible circuits are represented by a particular kind of $m \times m$ unitary matrices: the $m \times m$ permutation matrices. Such matrices may be decomposed the way described above. However, they may also be decomposed according to the Clos decomposition, based on Birkhoff's decomposition of doubly stochastic matrices: see Fig. 2b. Applying such matrix decomposition again and again leads to the circuit decomposition of Fig. 3b, with only $2w-1$ control gates. Each box in the figure denotes a controlled 1-bit transformation, i.e. a 2×2 permutation matrix. The actual matrix depends on the state of the other $w-1$ bits. Therefore the box, in fact, depicts 2^{w-1} matrices of size 2×2, each from the finite group $\mathbf{S}_2$. As this group consists of merely two members (the trivial follower and the inverter), the boxes may be regarded as NOT gates, the control gates thus being controlled NOTs.

The question arises whether computing schemes exist which are intermediate to classical and quantum. Such computations are represented by a matrix group X, that is simultaneously a subgroup of U(m) and a supergroup of $\mathbf{S}_m$:

$$\mathbf{S}_m \subset \mathrm{X} \subset \mathrm{U}(m) \ . \tag{1}$$

Such group may exist in three different kinds:

- either a finite group with order $D > m!$,
- or a discrete group with a countable infinity $\aleph_0$ as order,
- or a Lie group with dimension $d < m^2$.

Each of these possibilities deserves our attention. The larger X, the more difficult it is to implement it into hardware, but the more powerful is the resulting computer. Assuming that for a lot of interesting problems the quantum computer, based on the whole group U(m), is 'overkill', we have to look for a satisfactory compromise between simplicity (found close to $\mathbf{S}_m$) and computational power (found close to U(m)). Computers close to $\mathbf{S}_m$, we may refer to as 'reversible plus', whereas computers close to U(m), we may refer to as 'quantum light'.

We may tackle this problem in two ways: either bottom-up [1] or top-down [2]. For bottom-up, we start from the symmetric group and add some extra group generators. For top-down, we start from the unitary group and impose some restrictions.

II. Cosine-sine-like decomposition

Thanks to the cosine-sine decomposition of unitary matrices, any unitary computer can be decomposed as in Fig. 2a and thus to the cascade of Fig. 3a. Such decomposition has successfully been applied in quantum circuit synthesis [2] [3] [4] [5] [6] [7]. The question arises whether this is also true for other cases.

We consider $m\times m = 2^w \times 2^w$ matrices. If they form a Lie group X(m) of dimension d, then the decomposition according to Fig. 2a (with two boxes from X($m-1$) and one box from X(2)) is only possible provided

$$4\, d(\frac{m}{2}) + \frac{m}{2}\ d(2) \geq d(m) \ . \tag{2}$$

If the $m \times m$ matrices form a finite matrix group $\mathbf{X}_m$ of order D, then the necessary condition for the decomposition (with two boxes from $\mathbf{X}_{m-1}$ and one box from $\mathbf{X}_2$) is

$$\Big[D(\frac{m}{2})\Big]^4\ [D(2)]^{m/2} \geq D(m) \ . \tag{3}$$

This latter inequality reduces to the former one, by merely setting $d = \log(D)$. Thus, for both finite and infinite groups, we investigate the equation

$$d(m) = 4\, d(\frac{m}{2}) + \frac{m}{2}\ d(2) \ .$$

Introducing $f(w) = d(2^w)$, this becomes the recurrence relation

$$f(w) = 4\, f(w-1) + f(1) 2^{w-1} \ .$$

According to Appendix A (with $a = 4$, $b = f(1)/2$, and $c = 2$), its solution is:

$$f(w) = \frac{f(1)}{2}\ (4^w - 2^w)$$

or

$$d(m) = \frac{d(2)}{2}\ (m^2 - m) \ .$$

In order to fulfil inequality (2), the dimension $d(m)$ of the Lie group should grow with the degree m, according to $\frac{d(2)}{2}\ (m^2-m)$ or slower. The unitary group U(m) with dimension m^2 and the special unitary group SU(m) with dimension m^2-1 fulfil this condition. In order to obey inequality (3), the order $D(m)$ of the finite group should grow with the degree m, according to $[\ \sqrt{D(2)}\ ]^{m^2-m}$ or slower. The symmetric group $\mathbf{S}_m$ with order $m!$ fulfils this condition (as $m!$ grows like $(m/e)^m$, according to Stirling's formula).

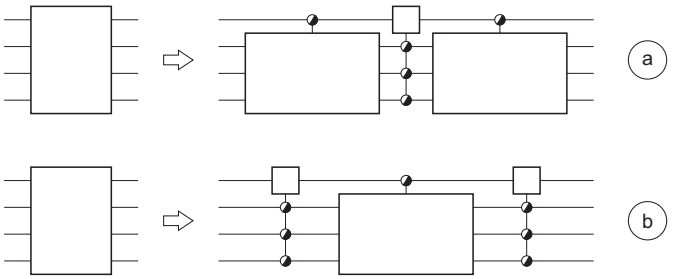

Fig. 2. Decomposition of a circuit into three parts: (a) a member of U(2^w) into two members of U(2^{w-1})^2 and one member of U(2)$^{2^{w-1}}$ and (b) a member of $\mathbf{S}_{2^w}$ into two members of $\mathbf{S}_2^{2^{w-1}}$ and one member of $\mathbf{S}_{2^{w-1}}^2$.

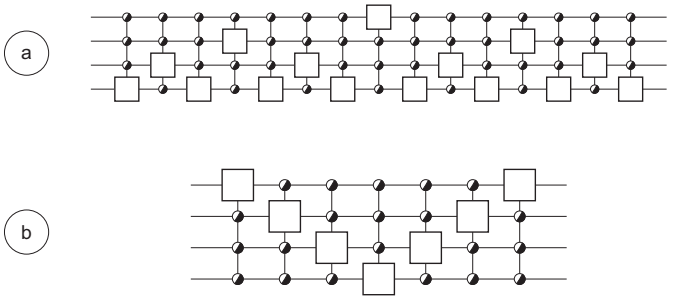

Fig. 3. Decomposition of a circuit (a) into 2^w-1 parts, each member of U(2)$^{2^{w-1}}$ and (b) into $2w-1$ parts, each member of $\mathbf{S}_2^{2^{w-1}}$.

III. Birkhoff-like decomposition

From the previous section, we have seen that not only the quantum computers (with transformations from U(m)), but also classical reversible computers (with transformations from $\mathbf{S}_m$) can profit from the decomposition of Fig. 2a. Thanks to the Birkhoff decomposition of doubly stochastic matrices, any reversible classical computer can also be decomposed as in Fig. 2b, leading to a far more efficient decomposition: Fig. 3b. Such decomposition has successfully been applied in (classical) reversible circuit synthesis [2] [8] [9]. The question arises whether this is also true for other cases.

We consider $m \times m = 2^w \times 2^w$ matrices. If they form a Lie group of dimension d, then the decomposition according to Fig. 2b is only possible provided

$$m\, d(2) + 2\, d(\frac{m}{2}) \geq d(m) \ . \tag{4}$$

If the $m \times m$ matrices form a finite matrix group of order D, then the necessary condition for decomposition is

$$[D(2)]^m \ \left[D(\frac{m}{2})\right]^2 \geq D(m) \ . \tag{5}$$

This latter inequality reduces to the former one, by merely setting $d = \log(D)$. Thus, for both finite and infinite groups, we investigate the equation

$$d(m) = 2\, d(\frac{m}{2}) + m\, d(2) \ .$$

Again applying $f(w) = d(2^w)$, this becomes the recurrence relation

$$f(w) = 2f(w-1) + f(1)2^w \ .$$

According to Appendix A (with $a = c = 2$ and $b = f(1)$), its solution is:

$$f(w) = f(1)\,(w - \frac{1}{2})\,2^w$$

or

$$d(m) = d(2)\ \left[\log_2(m) - \frac{1}{2}\right]\ m \ .$$

In order to fulfil inequality (4), the dimension $d(m)$ of the Lie group should grow with the degree m, according to $d(2)\,[\log_2(m) - 1/2\,]\,m$ or slower. The unitary group U(m) and the special unitary group SU(m) do not obey this condition. In order to fulfil inequality (5), the order $D(m)$ of the finite group should grow with the degree m, according to $[D(2)]^{[\log_2(m)-1/2]\,m}$ or slower. The symmetric group $\mathbf{S}_m$ fulfils this condition.

IV. Results

We consider a group of matrices of size $m \times m$. We define the function $\Phi(m)$:

- If the group is a Lie group of dimension $d(m)$, then

$$\Phi(m) = \frac{d(m)}{d(2)} \ .$$

- If the group is a finite group of order $D(m)$, then

$$\Phi(m) = \frac{\log D(m)}{\log D(2)} \ .$$

Table I gives some notorious group examples, ordered by decreasing Φ. For a group to be decomposable according to the cosine-sine scheme, it is necessary that

$$\Phi(m) \leq \frac{1}{2}\, m^2 - \frac{1}{2}\, m \ ; \tag{6}$$

for a group to be decomposable according to the Birkhoff scheme, it is necessary that

$$\Phi(m) \leq m \log_2(m) - \frac{1}{2}\, m \ . \tag{7}$$

We denote by $\Phi_1(m)$ and $\Phi_2(m)$ the right-hand sides of the eqns (6) and (7), respectively. The upper part of the table lists some groups that obey $\Phi_1(m) \geq \Phi(m) > \Phi_2(m)$ and thus may possibly be decomposed according to the cosine-sine scheme; the lower part of the table shows groups that obey $\Phi_2(m) > \Phi(m)$ and thus may possibly be decomposed according both to the cosine-sine scheme and to the Birkhoff scheme. Fig. 4 shows some $\Phi(m)$ curves, as well as the two boundaries $\Phi_1(m)$ and $\Phi_2(m)$.

TABLE I
SOME FAMOUS GROUPS AND THEIR Φ FUNCTION.

group name	notation	order $D(m)$	dimension $d(m)$	$\Phi(m)$
orthogonal	O(m)		$\frac{1}{2}(m^2-m)$	$\frac{1}{2}m^2-\frac{1}{2}m$
spec. unitary	SU(m)		m^2-1	$\frac{1}{3}m^2-\frac{1}{3}$
unitary	U(m)		m^2	$\frac{1}{4}m^2$
symmetric	$\mathbf{S}_m$	$m!$		$\log_2(m!)$
contr. NOT	$\mathbf{S}_2^{m/2}$	$2^{m/2}$		$\frac{1}{2}m$
controlled V	U(2)$^{m/2}$		$2m$	$\frac{1}{2}m$
cyclic	$\mathbf{Z}_m$	m		$\log_2(m)$
Pauli	$\mathbf{P}_m$	m^4		$\log_2(m)$

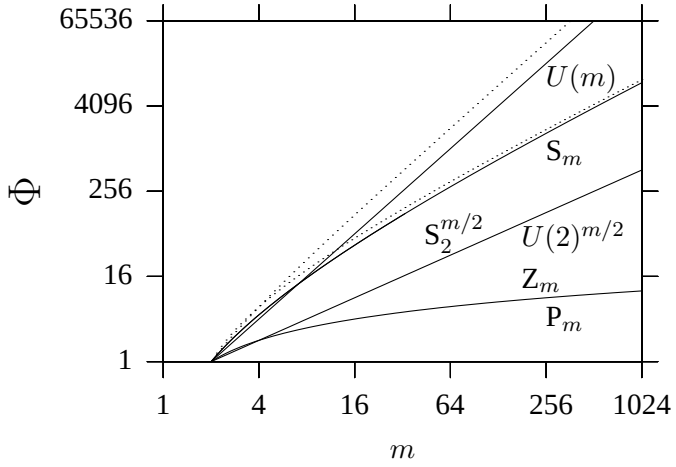

Fig. 4. The function $\Phi(m)$ of some well-known groups, i.e. the unitary group U(m), the symmetric group $\mathbf{S}_m$, the control groups $\mathbf{S}_2^{m/2}$ and U(2)$^{m/2}$, the cyclic group $\mathbf{Z}_m$, and the Pauli group $\mathbf{P}_m$. The two dotted curves show the critical borderline Φ_1 (upper dotted line) and the critical borderline Φ_2 (lower dotted line).

None of the well-known groups in Table I obeys $\Phi(m) > \Phi_1(m)$. Nevertheless such groups exist. Suffice it to give two examples:

- The even $m \times m$ permutation matrices form the alternating group $\mathbf{A}_m$ with order $D(m) = m!/2$. Because $D(2)$ equals 1, we have $\Phi(2) = 1$ and $\Phi(m) = \infty$ for all $m > 2$. We conclude that $\Phi(m) > \Phi_1(m)$. This is no surprise, as the only 2×2 alternating matrix is the 2×2 identity matrix. Thus all boxes in Fig. 3 are 'controlled followers'. Thus both circuits in the figure are w-(qu)bit identity circuits and thus cannot synthesize any of the other $m!/2 - 1$ alternating matrices.
- The unitary $m \times m$ matrices with all line sums (i.e. column sums and row sums) equal to 1 form a group with dimension $d(m) = m^2 - 2m + 1$ and thus $\Phi(m) = m^2 - 2m + 1 > \Phi_1(m)$. No matter how hard we try, we can never find a synthesis method leading to a decomposition according to either of the two schemes in Fig. 3.

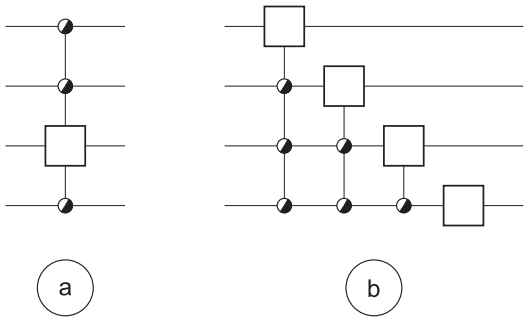

Fig. 5. Decomposition of a circuit (a) into 1 part, member of U(2)$^{2^{w-1}}$ and (b) into w parts, each member of $\mathbf{S}_2^{2^x}$, with x subsequently equal to $w-1$, $w-2$, ..., 1, and 0.

We stress that, if a group satisfies the necessary condition $\Phi(m) \leq \Phi_1(m)$, it is not proved that an actual decomposition according to Fig. 3a exists, as the condition is not sufficient. In order to find out whether a decomposition is really possible, each case should be investigated separately. In the same way, $\Phi(m) \leq \Phi_2(m)$ is a necessary but by no means a sufficient condition for a Birkhoff-style decomposition (Fig. 3b). We now give some examples of detailed investigations.

All controlled gates with the same controlled (qu)bit form a group. If the controlled gate is a NOT gate, then this group is finite, of the order $2^{2^{w-1}}$, isomorphic to $\mathbf{S}_2^{2^{w-1}}$, a subgroup of $\mathbf{S}_{2^w}$. According to Table I and Fig. 4 the members of this group might be decomposed according either to Fig. 3a or to Fig. 3b. Do such decompositions actually exist? Of course. We even can do much better: such gate is its own decomposition: we do not need to cascade $2^w - 1$ nor $2w-1$ building-blocks, as a single building-block is sufficient. Fig. 5a gives the 'decomposition', in case $w = 4$ and the controlled wire is the third wire. If the controlled gate is a V gate, i.e. a member of U(2), then the controlled V gates acting on the same qubit form a Lie group of dimension $4 \times 2^{w-1} = 2^{w+1}$, isomorphic to U(2)$^{2^{w-1}}$, a subgroup of U($2^w$). Again the 'decomposition' is trivial, according to Fig. 5a.

A somewhat less trivial example is the cyclic group $\mathbf{Z}_m$, a finite group of $m \times m$ permutation matrices, with order m. According to Table I and Fig. 4 the members of this group might be decomposed according either to Fig. 3a or to Fig. 3b. Do such decompositions exist? After some investigation, one finds out they do. One can even do better: each of the $m = 2^w$ members of the

group can be decomposed into w control gates, according to the scheme of Fig. 5b. As $\mathbf{Z}_2$ is the same as $\mathbf{S}_2$, the boxes represent NOT gates and thus we have a cascade of w controlled NOTs.

The examples of Fig. 5 have the disadvantage that they do not fulfil our goal (1). They are subgroups of U(2^w), but they are not supergroups of $\mathbf{S}_{2^w}$. Therefore, we construct a strategy creating automatically groups that do satisfy (1). For this purpose, we choose a group of 2×2 matrices that obeys

$$\mathbf{S}_2 \subset \mathrm{Y} \subset \mathrm{U}(2) \ .$$

We construct all possible control gates of logic width w and arbitrary controlled wire. This set does not form a group of its own. We consider it however as a set of generators, generating a group X which indeed automatically satisfies (1). We call X the creation of Y and we call Y the creator of X. So, whereas the creator is a group of 2×2 unitary matrices, the creation is a group of $2^w \times 2^w$ unitary matrices. E.g. $\mathbf{S}_{2^w}$ is created by $\mathbf{S}_2$, whereas U(2^w) is the creation of U(2). If Y is a finite group, then its creation X is a discrete group; if Y is a Lie group, then its creation X is also a Lie group.

As a first example, we discuss small creators: supergroups of $\mathbf{S}_2$ as small as possible, i.e. creators of order 4. There are only two ways to embed the group of follower and inverter in a group of order 4:

- either in one of two groups isomorphic to the cyclic group $\mathbf{Z}_4$
- or in a group isomorphic to the Klein Vierergruppe $\mathbf{V}$ which is isomorphic to $\mathbf{S}_2 \times \mathbf{S}_2$.

The two former supergroups $\mathbf{X}_2$ are generated by a single matrix:

$$\pm \frac{1}{2} \begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix} \ ,$$

i.e. ± 1 times the notorious 'square root of NOT' matrix [10] [11] [12] [13]. Each of the two groups, in turn, creates a family of groups $\mathbf{X}_m$ with the following orders [1]:

$$\begin{array}{rcll} \mathrm{order}(\mathbf{X}_m) & = & 4 & \text{if } m = 2, \text{ i.e. if } w = 1 \\ & & \aleph_0 & \text{if } m \geq 4, \text{ i.e. if } w \geq 2 \ . \end{array}$$

No cascade of a finite number of building-blocks can synthesize an infinite number of different circuits. Thus, for any $w \geq 2$, the two decompositions of Fig. 3 are impossible. This is confirmed by the infinite $\Phi(m)$ of $\mathbf{X}_m$.

The latter supergroup $\mathbf{X}_2$ of order 4 is generated by two matrices:

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ and } \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \ .$$

The group creates a family of groups $\mathbf{X}_m$ with orders $(m!)2^m/2$, such that

$$\Phi(m) = \frac{1}{2} \ \log_2(m!) + \frac{1}{2} \ m - \frac{1}{2} \ .$$

It consists of all $m \times m$ unitary matrices where all non-zero entries are either 1 or -1, with the restriction that the number of entries equal to -1 is even. We have $\Phi(m) < \Phi_2(m)$ and indeed each element of the group is Birkhoff-decomposable. A possible synthesis strategy is given in Appendix B.

Another example is the creation by the somewhat larger creator $\mathbf{P}_2$, i.e. the 1-qubit Pauli group of order 16 (generated by the three 2×2 Pauli matrices). The creation $\mathbf{X}_m$ is not $\mathbf{P}_m$, the Pauli group [14] of order $4 \times 4^w = 4m^2$, but instead a far larger group, of order $(m!)4^m/2$, such that

$$\Phi(m) = \frac{1}{4} \ \log_2(m!) + \frac{1}{2} \ m - \frac{1}{4} \ .$$

It consists of all $m \times m$ unitary matrices where all non-zero entries are either 1, or i, or -1, or $-i$, with the restriction that the number of entries equal to $\pm i$ is even. We have $\Phi(m) < \Phi_2(m)$ and indeed each element of the group is Birkhoff-decomposable. A possible synthesis strategy is given in Appendix C.

If the creator is a Lie group, we may distinguish three cases: either $d(2) = 3$, or $d(2) = 2$, or $d(2) = 1$. Condition (6) for cosine-sine decomposability becomes

$$\begin{array}{rcl} d(m) & \leq & \frac{3}{2} \ m^2 - \frac{3}{2} \ m \ , \\ d(m) & \leq & m^2 - m \ , \\ d(m) & \leq & \frac{1}{2} \ m^2 - \frac{1}{2} \ m \ , \end{array}$$

respectively. The first of these inequalities may be disregarded, as it is fulfilled automatically. Indeed, if the creator X(2) is unitary, then the creation X(m) is automatically unitary as well and thus obeys $d(m) \leq m^2$. Checking either of the two other conditions is not an easy task, as computing $d(m) = \dim[\mathrm{X}(m)]$ of the creation from the properties of the creator X(2) is not straightforward.

V. Conclusion

We have introduced a method to construct computation architectures, which are intermediate between classical computation and quantum computation. They are described by groups intermediate to the finite symmetric group and the unitary Lie group. For this purpose, we start from a group of 2×2 matrices, which is both

- a supergroup of the group consisting merely of the 2×2 identity matrix and the 2×2 NOT matrix, and

- a subgroup of the group of all 2×2 unitary matrices.

The former is isomorphic to the finite group $\mathbf{S}_2$ of order 2; the latter is isomorphic to the Lie group U(2) of dimension 4.

From such a group of 2×2 matrices (called the creator), a group of $2^w \times 2^w$ matrices (called the creation) is deduced. The created group can be of three different kinds:

- either a finite group,
- or a discrete group with a countable infinity as order,
- or a Lie group, i.e. a group with a non-countable infinity as order.

Each creation represents a different computer archtecture, with properties intermediate to classical reversible computation and quantum computation. Some of these architectures resemble either reversible computing or quantum computing. Some creations can e.g. be decomposed in a way either similar to the Birkhoff decomposition of classical computers or similar to the cosine-sine decomposition of quantum computers. Other archtectures, in particular those represented by groups of order $\aleph_0$, are quite new.

Appendix A
A recurrence equation

We investigate the recurrence relation

$$f(w) = a\, f(w-1) + b\, c^w \ .$$

First, we perform the substitution $f(w) = a^w r(w)$, leading to

$$r(w) = r(w-1) + b\, \left(\frac{c}{a}\right)^w \ .$$

We solve by adding the equations for $w = 2$, $w = 3$, etc.:

$$r(w) = r(1) + b\, \left[\, \left(\frac{c}{a}\right)^2 + \left(\frac{c}{a}\right)^3 + ... + \left(\frac{c}{a}\right)^w \,\right] \ .$$

Here, we have to distinguish between two cases: either $c = a$ or $c \neq a$.

Case $c \neq a$

By summing we obtain

$$r(w) = r(1) + \frac{bc^2}{a(c-a)}\, \left[\, \left(\frac{c}{a}\right)^{w-1} - 1 \,\right] \ .$$

Multiplying by a^w yields

$$f(w) = \frac{1}{a}\, \left[\, f(1) - \frac{bc^2}{c-a} \,\right]\, a^w + \frac{bc}{c-a}\, c^w \ .$$

Case $c = a$

By summing we obtain

$$r(w) = r(1) + (w-1)b \ .$$

Multiplying by a^w yields

$$f(w) = b\, w a^w + \left[\, \frac{f(1)}{a} - b \,\right]\, a^w \ .$$

Appendix B
A synthesis strategy

We consider any $m \times m$ unitary matrix with all entries from $\{0, 1, -1\}$, with the restriction that the number of entries equal to -1 is even. Such matrix can be decomposed into a product of an $m \times m$ permutation matrix and a diagonal matrix with diagonal elements from $\{1, -1\}$. The permutation matrix can be decomposed according to Fig. 2b [8]. The diagonal matrix can be positioned between the first and the second block of that figure (after the necessary permutation of its diagonal elements, because commuting a diagonal matrix with a permutation matrix rearranges the diagonal entries). Then we let the diagonal matrix get absorbed by the middle matrix. If the diagonal matrix has an even number of -1 entries in its upper half (and thus also an even number of -1 entries in its lower half), then the middle matrix becomes a member of $\mathbf{X}^2_{2^{w-1}}$ and we have succeeded in finding a decomposition. If, on the contrary, the diagonal matrix has an odd number of -1 entries in its upper half (and thus also an odd number of -1 entries in its lower half), then the newly generated middle matrix will not be a member of $\mathbf{X}^2_{2^{w-1}}$, because the two different blocks only absorb an odd number of -1. In order to resolve this issue, we can add, between the first and the middle matrix, a unity matrix, which can be written as the product of two identical diagonal matrices with all diagonal elements equal to 1, except for the elements on the 2^{w-1} th row and the 2^w th row, where we choose entries -1. Subsequently, we let the right diagonal matrix be absorbed by the middle matrix and the left diagonal matrix be absorbed by the first matrix. By doing so, we turn the first matrix into a member of $\mathbf{S}_2^{2^{w-1}-1} \times \mathbf{V}$ and the middle matrix into a member of $\mathbf{X}^2_{2^{w-1}}$. Here $\mathbf{V}$ denotes the Klein group. By applying this procedure $w-1$ times, we succeed in finding a Birkhoff-like decomposition of $\mathbf{X}_{2^w}$ into $2w-1$ blocks of $\mathbf{V}^{2^{w-1}}$, since $\mathbf{S}_2 \subset \mathbf{V}$. To be more specific, our original circuit, member of $\mathbf{X}_{2^w}$ is decomposed into $2w-1$ blocks: one block from $\mathbf{S}_2^{2^{w-1}-1} \times \mathbf{V}$, one from $\mathbf{S}_2^{2^{w-1}-2} \times \mathbf{V}^2$, ..., one from $\mathbf{S}_2^{2^{w-1}-2^{w-2}} \times \mathbf{V}^{2^{w-2}}$, one block from $\mathbf{V}^{2^{w-1}}$, and $w-1$ blocks from $\mathbf{S}_2^{2^{w-1}}$.

APPENDIX C
ONE MORE SYNTHESIS STRATEGY

We consider any $m \times m$ unitary matrix with all entries from $\{0, 1, i, -1, -i\}$, with the restriction that the number of entries equal to $\pm i$ is even. Such matrix can be decomposed into a product of an $m \times m$ permutation matrix and a diagonal matrix with diagonal elements from $\{1, i, -1, -i\}$. We proceed as in Appendix B, decomposing the permutation matrix in the Birkhoff way and positioning the diagonal matrix between the first and the second block (after the necessary rearrangement of its diagonal elements). If the diagonal matrix has an even number of $\pm i$ entries in its upper half (and thus also an even number of $\pm i$ entries in its lower half), it simply gets absorbed by the middle block of Fig. 2b. If, on the contrary, the diagonal matrix has an odd number of $\pm i$ entries in its upper half (and thus also an odd number of $\pm i$ entries in its lower half), then we can add the unity matrix, written as the product of two identical diagonal matrices with all diagonal elements equal to 1, except for the elements on the 2^{w-1} th row and the 2^w th row, where we choose entries $-i$ and i for one matrix and i and $-i$ for the other. One matrix gets absorbed by the middle matrix, the other by the first matrix. As a result, our original circuit, member of $\mathbf{X}_{2^w}$, is decomposed into three blocks: one member of $\mathbf{S}_2^{2^{w-1}-1} \times \mathbf{D}$, one member of $\mathbf{X}_{2^{w-1}}^2$, and one member of $\mathbf{S}_2^{2^{w-1}}$. Here $\mathbf{D}$ denotes the group generated by

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ and } \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} ,$$

i.e. by two of the three Pauli matrices. It is isomorphic to the dihedral group of order 8. If we proceed $w-1$ times like this, the original circuit, member of $\mathbf{X}_{2^w}$, is decomposed into $2w-1$ blocks: one block from $\mathbf{S}_2^{2^{w-1}-1} \times \mathbf{D}$, one from $\mathbf{S}_2^{2^{w-1}-2} \times \mathbf{D}^2$, ..., one from $\mathbf{S}_2^{2^{w-1}-2^{w-2}} \times \mathbf{D}^{2^{w-2}}$, one block from $\mathbf{P}_2^{2^{w-1}}$, and $w-1$ blocks from $\mathbf{S}_2^{2^{w-1}}$. All these blocks belong to $\mathbf{P}_2^{2^{w-1}}$, since $\mathbf{S}_2 \subset \mathbf{P}_2$ as well as $\mathbf{D} \subset \mathbf{P}_2$.

REFERENCES

[1] A. De Vos, J. De Beule, and L. Storme : " Computing with the square root of NOT ", *Serdica Journal of Computing*, vol. 3 (2009), pp. 359–370.

[2] A. De Vos and S. De Baerdemacker : " Reversible logic circuits versus quantum logic circuits ", *Advances in Mathematics of Communications*, submitted.

[3] M. Möttönen, J. Vartiainen, V. Bergholm, and M. Salomaa : " Quantum circuits for general multi-qubit gates ", *Physical Review Letters*, vol. 93 (2004), 130502.

[4] V. Bergholm, J. Vartiainen, M. Möttönen, and M. Salomaa : " Quantum circuits with uniformly controlled one-qubit gates ", *Physical Review A*, vol. 71 (2005), 052330.

[5] F. Khan and M. Perkowski : " Synthesis of ternary quantum logic circuits by decomposition ", *Proceedings of the 7 th International Symposium on Representations and Methodology of Future Computing Technologies*, Tokyo (September 2005), pp. 114–118.

[6] A. Slepoy : " Quantum gate decomposition algorithms ", *Sandia Report*, no. SAND2006-3440 (2006).

[7] V. Shende, S. Bullock, and I. Markov : " Synthesis of quantum-logic circuits ", *I.E.E.E. Transactions on Computer-aided Design of Integrated Circuits and Systems*, vol. 25 (2006), pp. 1000–1010.

[8] A. De Vos and Y. Van Rentergem : " Young subgroups for reversible computers ", *Advances in Mathematics of Communications*, vol. 2 (2008), pp. 183–200.

[9] A. De Vos and Y. Van Rentergem : " Multiple-valued reversible logic circuits ", *Journal of Multiple-Valued Logic and Soft Computing*, vol. 15 (2009), pp. 489–505.

[10] D. Deutsch : " Quantum computation ", *Physics World*, vol. 5 (June 1992), pp. 57–61.

[11] D. Deutsch, A. Ekert, and R. Lupacchini : " Machines, logic and quantum physics ", *The Bulletin of Symbolic Logic*, vol. 3 (2000), pp. 265–283.

[12] A. Galindo and M. Martín-Delgado : " Information and computation: classical and quantum aspects ", *Review of Modern Physics*, vol. 74 (2002), pp. 347–423.

[13] R. Wille and R. Drechsler : " Effect of BDD optimization on synthesis of reversible and quantum logic ", *Proceedings of the Workshop on Reversible Computation*, special session at the *2009 European Joint Conference on Theory and Practice of Software*, York, March 2009, *Electronic Notes in Theoretical Computer Science*, vol. 253 (2010), pp. 57–70.

[14] M. Nielsen and I. Chuang : " Quantum computation and quantum information ", Cambridge University Press (2000), pp. 454 and 611.